(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년07월29일
(11) 등록번호 10-2004196
(24) 등록일자 2019년07월22일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04W 12/06* (2009.01)
(21) 출원번호 10-2011-0145394
(22) 출원일자 2011년12월29일
심사청구일자 2016년12월15일
(65) 공개번호 10-2013-0076949
(43) 공개일자 2013년07월09일
(56) 선행기술조사문헌
JP2010278862 A*
KR1020000012607 A*
KR1020060102456 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
이일구
경기도 과천시 장군마을1길 62, 102호 (주암동, 청도주택)
(72) 발명자
이일구
광주광역시 광산구 월계로 117-32 105동 502호 (월계동,라인1차아파트)
(74) 대리인
특허법인인벤싱크

전체 청구항 수 : 총 4 항 심사관 : 양종필

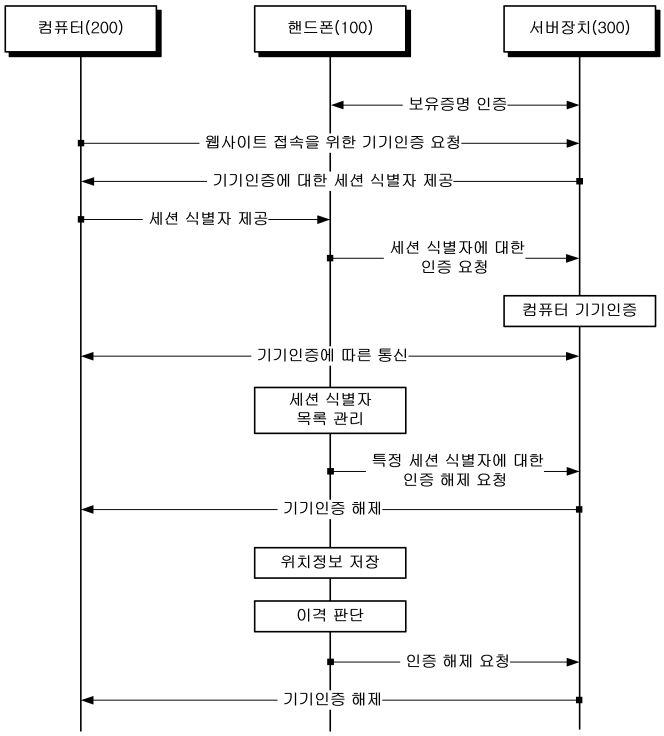
(54) 발명의 명칭 **로그인 세션 전달을 이용한 기기인증 방법**

(57) 요 약

본 발명은 단말장치 간에 로그인 세션을 전달함으로써 기기인증을 달성하는 기술에 관한 것이다. 특히, 본 발명은 보유증명 인증이 가능한 제 1 단말장치가 마련된 상태에서 제 1 단말장치와 통신이 가능한 제 2 단말장치에 대해 기기인증을 수행하고자 할 때, 제 2 단말장치의 기기인증을 위한 로그인 세션을 제 1 단말장치로 전달함으

(뒷면에 계속)

대 표 도 - 도1



로써 제 1 단말장치의 보유증명 인증에 기초하여 제 2 단말장치의 기기인증을 달성하는 기술을 제공한다. 본 발명의 로그인 세션 전달을 이용한 기기인증 방법에 따르면, 보유증명 인증이 가능한 단말장치(예: 핸드폰, 스마트폰)가 있다면 개인용 컴퓨터나 공용 컴퓨터를 비롯한 임의의 다른 단말에서도 개인정보를 보관하거나 노출할 위험없이 로그인을 손쉽게 달성할 수 있는 장점이 있다. 또한, 본 발명에 따르면 보유증명 인증이 가능한 단말장치를 통해 다른 단말의 기기인증을 원격 제어할 수 있고 나아가 보유증명 인증이 가능한 단말장치가 일정 이상 이동하면 다른 단말에서의 기기인증이 자동적으로 해제되도록 함으로써 로그인 상태의 단말을 제 3 자가 무단으로 사용하는 위험성을 방지할 수 있게되는 장점도 있다.

명 세 서

청구범위

청구항 1

이동통신 단말기가 서버장치에 대해 보유증명 인증을 수행하는 단계;

범용 컴퓨터가 상기 서버장치로 기기인증을 요청하는 단계;

상기 서버장치가 상기 범용 컴퓨터로 상기 기기인증에 대한 세션 식별자를 제공하는 단계;

상기 세션 식별자가 상기 이동통신 단말기로 제공되면 상기 이동통신 단말기가 상기 서버장치로 상기 세션 식별자에 대한 인증을 요청하는 단계; 및

상기 세션 식별자에 대한 인증을 요청한 상기 이동통신 단말기가 상기 보유증명 인증이 이루어진 것에 의해 상기 서버장치가 상기 세션 식별자에 대응하는 상기 범용 컴퓨터에 대한 기기인증을 실행하여 상기 세션 식별자에 대한 로그인이 이루어지는 단계;를 포함하고,

상기 이동통신 단말기의 화면 상에 상기 범용 컴퓨터에 의해 현재 로그인이 이루어진 세션 식별자의 목록을 표시하는 단계;

사용자에 의해서 상기 세션 식별자의 목록 중 특정 세션 식별자에 대한 인증 해제가 선택되면 상기 이동통신 단말기가 상기 특정 세션 식별자에 대한 인증 해제를 상기 서버 장치로 요청하는 단계; 및

상기 특정 세션 식별자에 대한 로그인이 이루어진 범용 컴퓨터가 상기 특정 세션 식별자에 대한 로그아웃을 처리하도록 상기 서버 장치가 상기 특정 세션 식별자에 대응하는 기기인증을 해제하는 단계를 더 포함하여 구성되는 로그인 세션 전달을 이용한 기기인증 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 이동통신 단말기가 상기 세션 식별자에 대한 인증을 요청한 당시의 상기 이동통신 단말기의 등록 위치를 등록하는 단계;

상기 이동통신 단말기가 현재 위치와 상기 등록 위치 간의 이격 거리를 획득하는 단계;

상기 이격 거리가 미리 설정된 임계치 이상인지 판단하는 단계;

상기 판단 결과, 상기 이격 거리가 상기 임계치 이상인 경우 상기 이동통신 단말기가 상기 등록 위치에 대응되는 세션 식별자에 대한 인증해제를 상기 서버장치로 요청하는 단계; 및

상기 서버장치가 상기 해제요청된 세션 식별자에 대응하는 기기인증을 해제하는 단계;를 더 포함하여 구성되는 로그인 세션 전달을 이용한 기기인증 방법.

청구항 4

제3항에 있어서,

상기 보유증명 인증을 수행하는 단계는, 상기 서버장치가 상기 이동통신 단말기의 가입정보에 기초하여 상기 보유증명 인증을 수행하는 것을 특징으로 하는 로그인 세션 전달을 이용한 기기인증 방법.

청구항 5

제4항에 있어서, 상기 이동통신 단말기가 상기 서버장치로 상기 세션 식별자에 대한 인증을 요청하는 단계는,

상기 범용 컴퓨터가 메세징 통신을 통해 상기 세션 식별자를 상기 이동통신 단말기로 전송하는 단계를 포함하여

구성되는 것을 특징으로 하는 로그인 세션 전달을 이용한 기기인증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 단말장치 간에 로그인 세션을 전달함으로써 기기인증을 달성하는 기술에 관한 것이다. 특히, 본 발명은 보유증명 인증이 가능한 제 1 단말장치가 마련된 상태에서 제 1 단말장치와 통신이 가능한 제 2 단말장치에 대해 기기인증을 수행하고자 할 때, 제 2 단말장치의 기기인증을 위한 로그인 세션을 제 1 단말장치로 전달함으로써 제 1 단말장치의 보유증명 인증에 기초하여 제 2 단말장치의 기기인증을 달성하는 기술을 제공한다.

배 경 기 술

[0002] 현재 사용자들은 다양한 인터넷 접속도구를 통하여 인터넷 서비스를 이용하고 있다. 사용자의 집 또는 회사의 개인용 컴퓨터뿐만 아니라 휴대용 단말(예: 휴대폰, 스마트폰, 스마트패드, PDA, 와이브로단말 등)을 이용한 인터넷 이용도 폭발적으로 증가하고 있는 추세이다.

[0003] 그러나, 사용자는 서비스 제공자가 제공하는 서비스를 제공받기 위해서 자기가 가입한 사이트를 기억하는 것뿐만 아니라 자신의 사용자 ID와 비밀번호를 기억해야 하는 어려움이 존재한다. 이러한 문제로 인해 사용자가 동일한 ID와 비밀번호를 여러 사이트에 동일하게 사용하는 문제가 발생한다. 기억하기 쉽다는 이유만으로 동일한 사용자 ID와 비밀번호를 사용하는 것은 온라인에서 개인정보를 쉽게 도용당하는 구실을 제공한다. 특정 사이트에서 개인정보가 유출된 경우, 그 개인정보는 다른 사이트에서 이용될 수가 있고, 이로 인해 사용자는 예상치 못한 심각한 피해를 받을 수 있게 된다.

[0004] 한편, 공용 단말(예: 인터넷 카페나 공공 장소의 공용컴퓨터)의 경우, 높은 컴퓨팅 파워와 고해상도 디스플레이가 필요한 경우에 공공 장소에서 종종 사용되는 경우가 있다. 하지만, 공공 장소의 경우 보안상 취약한 점이 많이 있기 때문에 공용 단말을 이용하여 서비스 제공자가 제공하는 인터넷 서비스를 제공받을 때, 개인정보(예: 사용자 ID, 비밀번호)를 입력하는 과정에서 피싱이나 해킹 등으로 사용자의 개인 정보가 유출될 수 있는 여지가 많다.

[0005] 이러한 단점을 보완하기 위하여, 웹 브라우저(Web browser)가 이전에 입력된 비밀번호를 자동 입력해 준다거나, 사용자가 공용 단말을 사용할 때 모바일 단말에 임시 인증코드를 전달하여 전달된 인증코드로 사용자를 인증하는 방법 등이 제시되었다. 하지만, 상기한 방법의 경우 시스템적으로 전술한 문제점을 근본적으로 해결하였다고 보기 어려웠다.

[0006] 다른 방법으로는 인증정보(예: 서버 URL과 비밀번호 등)를 스마트카드 등과 같은 물리적인 보안매체에 저장하여 여러 개인 단말에서 서버 접근을 가능하도록 하는 방법이 있는데, 이는 하드웨어 장치를 추가로 요구할 뿐만 아니라 해당 인증정보가 노출되는 문제가 여전히 발생한다.

[0007] 한편, 최근 휴대용 단말을 이용해 일반 인터넷 서비스와 동일한 형태로 문서나 동영상을 볼 수 있는 서비스인 '풀브라우징(Full Browsing)'의 성능이 개선되면서, 휴대용 단말을 이용한 무선 인터넷 시장이 급속도로 성장하고 있다. 하지만, 사용자들은 휴대용 단말을 통해 인터넷 서비스를 제공받기 위해서 복잡한 방법으로 사용자 등록 및 인증을 수행해야만 했다. 이에, 휴대용 단말을 이용한 무선 인터넷 서비스를 활성화하고 보편화하기 위해서는 휴대용 단말을 이용하여 사용자가 친숙한 인터페이스를 통해 사용자 등록 및 인증을 수행할 수 있는 방법이 필요한 실정이다.

[0008] 한편, 하나의 단말장치 안에서 인증 과정으로 주로 쓰이는 것은 종래로부터 비밀번호 입력 방식이다. 비밀번호를 입력하는 일은 사용자에게 때로는 매우 번거로워서 사용자는 자동 로그인 설정을 해두곤 한다. 보안을 더 확실하게 하기 위한 방법으로 다른 장치를 동원하는 방법도 있는데, 현재 원타임 패스워드가 널리 활용되고 있다. 이것 또한 원타임 패스워드 기기의 결과를 다른 장치에 사용자가 입력해야 하므로 번거롭다. 종래기술 중에는 휴대폰의 장치 정보를 이용해서 사용자를 인증한다는 발명이 있지만, 이것은 통신사의 도움을 받거나 휴대폰의 개인정보를 공개해야 하는 단점이 있다.

[0009] 다른 한편으로는 사용자가 일단 로그인을 수행한 다음에는 명시적으로 로그아웃을 하기 전까지는 로그인 상태가 계속 유지되고 있어 제 3 자에 의한 무단도용의 위험성이 존재하였다. 예를 들어, 사용자가 회사 인트라넷을

사용하여 업무를 보는 도중에 잠시 자리를 비운 동안, 그 로그인 상태로 유지되고 있는 단말장치(컴퓨터)를 제 3 자가 무단으로 사용할 위험성이 존재하는 것이다. 이러한 위험성을 해소할 목적으로 현재 다수의 은행사이트에서는 로그인된 상태로 일정 시간동안 아무런 액션이 없으면 자동 로그아웃시키는 기술을 적용하고 있으나, 그 일정 시간이 경과할 때까지는 여전히 보안공백이 존재하며, 더욱이 제 3 자가 무단으로 사용할 때에는 오히려 마우스 조작과 같은 액션이 계속 제공되므로 이러한 상황에 대해서는 아무런 해결책이 되지 못한다.

[0010] 이처럼 사용자가 이용하는 여러 장치에서 로그인을 수행하는 것은 다양한 문제점을 가지고 있으며, 이에 관해 보안을 강화하는 다양한 방법이 기존에 제안되었지만 문제점을 제대로 해결해주지 못하였담. 그에 따라 전술한 바와 같은 종래기술의 여러 문제점을 해소할 수 있는 기술의 개발이 관련 분야에서 오래 전부터 요망되고 있는 실정이다.

발명의 내용

해결하려는 과제

[0011] 본 발명의 목적은 단말장치 간에 로그인 세션을 전달함으로써 기기인증을 달성하는 기술을 제공하는 것이다. 특히, 보유증명 인증이 가능한 제 1 단말장치가 마련된 상태에서 제 1 단말장치와 통신이 가능한 제 2 단말장치에 대해 기기인증을 수행하고자 할 때, 제 2 단말장치의 기기인증을 위한 로그인 세션을 제 1 단말장치로 전달함으로써 제 1 단말장치의 보유증명 인증에 기초하여 제 2 단말장치의 기기인증을 달성하는 기술을 제공하고자 한다.

과제의 해결 수단

[0012] 이러한 목적을 달성하기 위하여, 본 발명에 따른 로그인 세션 전달을 이용한 기기인증 방법은, 제 1 단말장치(100)가 서버장치(300)에 대해 보유증명 인증을 수행하는 제 1 단계; 제 2 단말장치(200)가 서버장치(300)에 대해 기기인증을 요청하는 제 2 단계; 서버장치(300)가 제 2 단말장치(200)로 기기인증에 대한 세션 식별자를 제공하는 제 3 단계; 제 1 단말장치(100)가 세션 식별자를 제공받는 제 4 단계; 제 1 단말장치(100)가 서버장치(300)에 대해 보유증명 인증에 기초하여 세션 식별자에 대한 인증을 요청하는 제 5 단계; 서버장치(300)가 세션 식별자에 기초하여 제 2 단말장치(200)에 대한 기기인증을 실행하는 제 6 단계;를 포함하여 구성된다.

[0013] 이때, 본 발명에 따른 로그인 세션 전달을 이용한 기기인증 방법은, 제 1 단말장치(100)가 제 5 단계에서 인증을 요청한 세션 식별자의 목록을 관리하는 제 7 단계; 제 1 단말장치(100)가 목록에 포함된 특정의 세션 식별자에 대한 인증해제를 서버장치(300)에 대해 요청하는 제 8 단계; 서버장치(300)가 해제요청된 세션 식별자에 대응하는 기기인증을 해제하는 제 9 단계;를 더 포함하여 구성되는 것이 바람직하다.

[0014] 또한, 본 발명에 따른 로그인 세션 전달을 이용한 기기인증 방법은, 제 1 단말장치(100)가 5 단계에서 인증을 요청한 당시의 제 1 단말장치(100)의 위치정보를 저장하는 제 10 단계; 제 1 단말장치(100)가 현재의 위치가 제 10 단계에서의 위치로부터 미리 설정된 거리 이상 이격되었는지 여부를 판단하는 제 11 단계; 판단 결과, 미리 설정된 거리 이상 이격된 경우에는 제 1 단말장치(100)가 이격된 인증 요청에 대응하는 세션 식별자에 대한 인증해제를 서버장치(300)에 대해 요청하는 제 12 단계; 서버장치(300)가 해제요청된 세션 식별자에 대응하는 기기인증을 해제하는 제 13 단계;를 더 포함하여 구성될 수 있다.

[0015] 본 발명에서, 제 1 단말장치(100)는 이동통신 단말기(핸드폰)로 구현되고, 제 1 단계에서 서버장치(300)는 이동통신 단말기의 가입정보에 기초하여 보유증명 인증을 수행하는 것이 바람직하다. 또한, 제 4 단계는 제 2 단말장치(200)가 메세징 통신을 통해 세션 식별자를 제 1 단말장치(100)로 전송하는 단계를 포함하여 구성되는 것이 바람직하다.

발명의 효과

[0016] 본 발명의 로그인 세션 전달을 이용한 기기인증 방법에 따르면, 보유증명 인증이 가능한 단말장치(예: 핸드폰, 스마트폰)가 있다면 개인용 컴퓨터나 공용 컴퓨터를 비롯한 임의의 다른 단말에서도 개인정보를 보관하거나 노

출할 위험없이 로그인을 손쉽게 달성할 수 있는 장점이 있다.

[0017] 또한, 본 발명에 따르면 보유증명 인증이 가능한 단말장치를 통해 다른 단말의 기기인증을 원격 제어할 수 있고 나아가 보유증명 인증이 가능한 단말장치가 일정 이상 이동하면 다른 단말에서의 기기인증이 자동적으로 해제되도록 함으로써 로그인 상태의 단말을 제 3 자가 무단으로 사용하는 위험성을 방지할 수 있게되는 장점도 있다.

도면의 간단한 설명

[0018] [도 1]은 본 발명에 따른 로그인 세션 전달을 이용한 기기인증 방법의 전체 흐름을 나타낸 도면.

[도 2]는 본 발명에서 기기인증이 이루어지는 과정을 나타낸 순서도.

[도 3]은 본 발명에서 기기인증이 해제되는 일 실시예를 나타낸 순서도.

[도 4]는 본 발명에서 기기인증이 해제되는 다른 실시예를 나타낸 순서도.

발명을 실시하기 위한 구체적인 내용

[0019] 이하에서는 도면을 참조하여 본 발명을 상세하게 설명한다.

[0020] [도 1]은 본 발명에 따른 로그인 세션 전달을 이용한 기기인증 방법의 전체 흐름을 나타낸 도면이고, [도 2]는 본 발명의 기기인증 방법에서 컴퓨터(200)와 서버장치(300) 간에 핸드폰(100)을 매개로 기기인증이 이루어지는 과정을 나타낸 순서도이다. [도 1]과 [도 2]를 참조하여 기기인증이 이루어지는 과정을 설명하면 다음과 같다.

[0021] 먼저, 핸드폰(100)이 서버장치(300)에 대해 보유증명 인증을 수행하는 절차를 수행한다(S11). 본 발명에서 핸드폰(100)은 보유증명의 인증이 가능한 단말장치의 일 예로서 제시된 것으로, 핸드폰(이동통신 단말기)의 경우에는 서비스 가입할 때 각종의 정보를 제공할 뿐만 아니라 다른 경로를 통해 보유 정보를 검증받는 것이 가능하므로 보유증명의 인증이 가능하다. 사용자가 핸드폰(100)으로 특정 웹사이트를 액세스함으로써 당해 웹사이트를 관리하는 서버장치(300)에 대해 본 발명에 따른 보유증명 인증을 요청하고, 그 요청에 대응하여 서버장치(300)는 당해 핸드폰(100)에 대해 보유증명을 인증한다.

[0022] 이어서, 사용자가 컴퓨터(200)를 통해 위의 웹사이트를 접속하여 그 웹사이트를 관리하는 서버장치(300)에 대해 기기인증을 요청한다(S12). 웹사이트 로그인 과정을 수행하는 것이 기기인증 요청의 일 예이다.

[0023] 그에 대해, 서버장치(300)는 컴퓨터(200)로 당해 기기인증에 대한 세션 식별자(예: #328)를 제공한다(S13). 세션 식별자는 사용자가 디스플레이 화면으로 확인할 수 있는 방식으로 제공할 수도 있고, 화면 상에서는 표시되지 않으면서 내부 데이터로서 제공될 수도 있다.

[0024] 그리고 나서, 핸드폰(100)이 세션 식별자를 제공받는다(S14). 컴퓨터(200)가 예컨대 일종의 메세징 통신을 통해서 세션 식별자를 핸드폰(100)으로 전달할 수도 있고, 아니면 다소 불편하지만 사용자가 핸드폰(100)의 키패드를 사용하여 세션 식별자를 입력해주는 것도 가능하다.

[0025] 이어서, 핸드폰(100)은 서버장치(300)에 대해 앞서 실행한 보유증명 인증에 기초하여 세션 식별자에 대한 인증을 요청한다(S15). 핸드폰(100)은 위 제공받은 세션 식별자(예: #328)를 서버장치(300)로 제공하여 인증을 요청하는데, 그 전에 보유증명 인증이 이루어진 상태이므로 세션 식별자에 대한 인증이 서버장치(300)에 의해 받아들여질 것으로 기대한다.

[0026] 서버장치(300)는 보유증명 인증이 이루어진 핸드폰(100)으로부터 요청된 세션 식별자 인증 요청을 받아들이고, 그에 따라 당해 세션 식별자에 대응되는 기기인증 요청, 즉 컴퓨터(200)에 대한 기기인증 요청을 받아들인다(S16). 그에 따라 서버장치(300)가 관리하는 웹사이트에 대해서 컴퓨터(200)의 기기인증(로그인)이 이루어지는 것이다.

[0027] 기기인증이 이루어짐에 따라 컴퓨터(200)와 서버장치(300) 간에 정상적인 통신이 실행된다(S17). 즉, 로그인이 성공됨에 따라 컴퓨터(200)는 당해 웹사이트를 로그인한 상태로 자유롭게 이용할 수 있게 되는 것이다. 바람직하게는 하나의 핸드폰(100)을 통해서 복수의 컴퓨터(200)에 대해 각각 상이한 서버장치(300)로 기기인증을 달성할 수 있다.

[0028] [도 3]은 본 발명에서 앞서 이루어진 기기인증이 해제되는 일 실시예를 나타낸 순서도이다. [도 1]과 [도 3]을 참조하여 본 발명에서 기기인증이 해제되는 일 과정을 설명하면 다음과 같다.

[0029] 먼저, 핸드폰(100)은 보유증명 인증을 매개로 세션 식별자에 대한 인증을 서버장치(300)로 요청하는데, 핸드폰(100)은 이렇게 인증을 요청한 세션 식별자의 목록을 관리한다(S21).

[0030] 그에 따라 핸드폰(100)의 사용자는 핸드폰(100)의 예컨대 화면 상에서 그 목록에 관한 정보(예: 현재 로그인이 이루어진 웹사이트 리스트)를 확인할 수 있는데, 이 목록에 포함된 특정의 웹사이트에 대한 인증해제(예: 로그아웃)를 선택하면 그에 따라 핸드폰(100)은 당해 세션 식별자에 대한 인증해제를 서버장치(300)에 대해 요청한다(S22).

[0031] 핸드폰(100)에 세션 식별자에 대한 인증해제를 요청함에 따라 서버장치(300)는 당해 세션 식별자에 대응하는 기기인증을 해제하고(S23), 그에 따라 당해 컴퓨터(200)는 강제로 로그아웃 처리된다.

[0032] [도 4]는 본 발명에서 앞서 이루어진 기기인증이 해제되는 다른 실시예를 나타낸 순서도이다. [도 1]과 [도 4]를 참조하여 본 발명에서 기기인증이 해제되는 다른 과정을 설명하면 다음과 같다.

[0033] 먼저, 핸드폰(100)은 앞서 세션 식별자에 대한 인증을 요청할 당시의 자신의 위치정보를 저장한다(S31).

[0034] 그리고 나서, 핸드폰(100)은 현재 자신의 위치와 그 등록 위치 간의 이격 거리를 지속적으로 모니터링하며(S32), 그 이격 거리가 미리 설정된 임계치를 초과하는지 여부를 판단한다(S33).

[0035] 단계(S33)의 판단 결과 이격 거리가 임계치를 초과하는 경우에는, 사용자가 컴퓨터(200)를 로그인해둔 상태에서 자리를 벗어난 것으로 간주하고 핸드폰(100)은 당해 컴퓨터(200)에 대해 강제적인 인증해제를 시도한다. 즉, 핸드폰(100)이 그 이격된 등록 위치에 대응되는 세션 식별자에 대한 인증해제를 서버장치(300)에 대해 요청하며(S34), 서버장치(300)는 핸드폰(100)으로부터 인증해제 요청이 이루어진 세션 식별자에 대응하는 기기인증을 해제한다(S35). 이 경우에도 당해 컴퓨터(200)는 강제로 로그아웃 처리된다.

[0036] 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드의 형태로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0037] 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기테이프, 플로피 디스크, 광 데이터 저장장치 등이 있으며, 캐리어웨이브(예컨대, 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산된 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인 프로그램, 코드, 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

[0038] 이상과 같이, 본 명세서와 도면에는 본 발명의 실시예에 대하여 개시하였으며, 비록 특정 용어들이 사용되었으나 이는 단지 본 발명의 기술 내용을 쉽게 설명하고 발명의 이해를 돕기 위한 일반적인 의미에서 사용된 것이지, 본 발명의 범위를 한정하고자 하는 것은 아니다. 여기에 개시된 실시예 외에도 본 발명의 기술적 사상에 바탕을 둔 다른 변형예가 가능하다는 것은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 자명하다.

부호의 설명

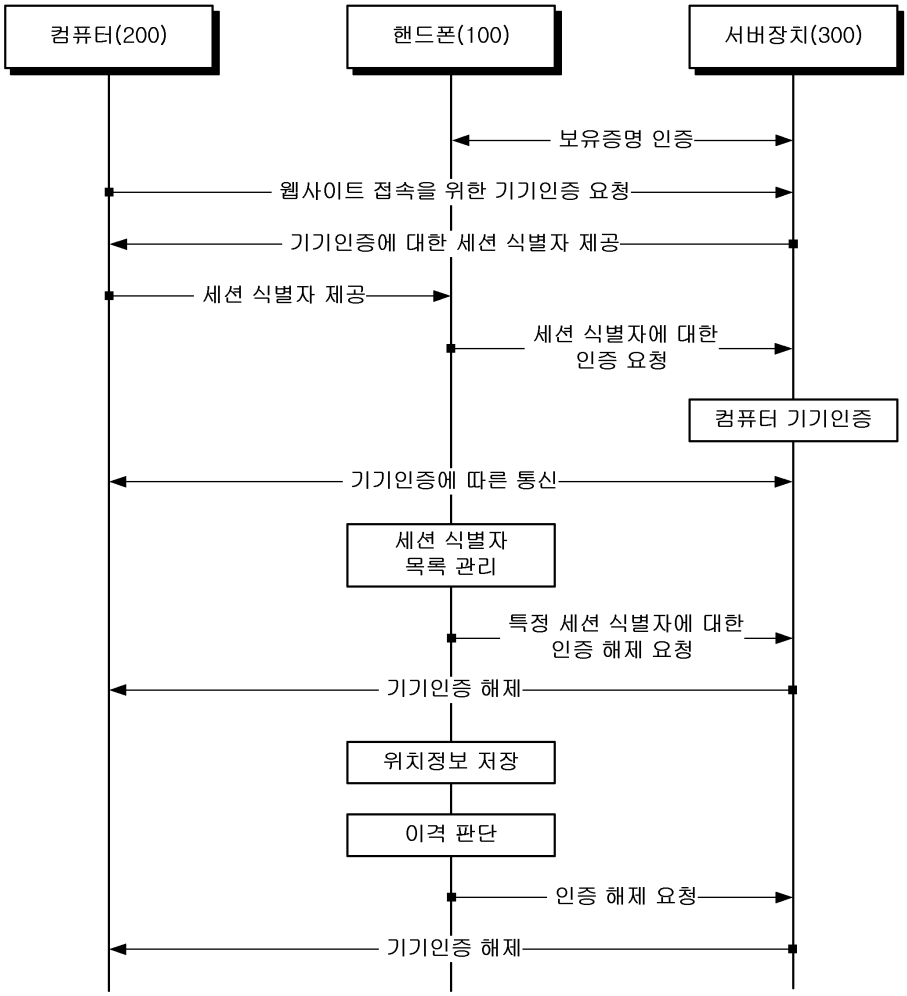
[0039] 100: 제 1 단말장치(핸드폰)

200: 제 2 단말장치(컴퓨터)

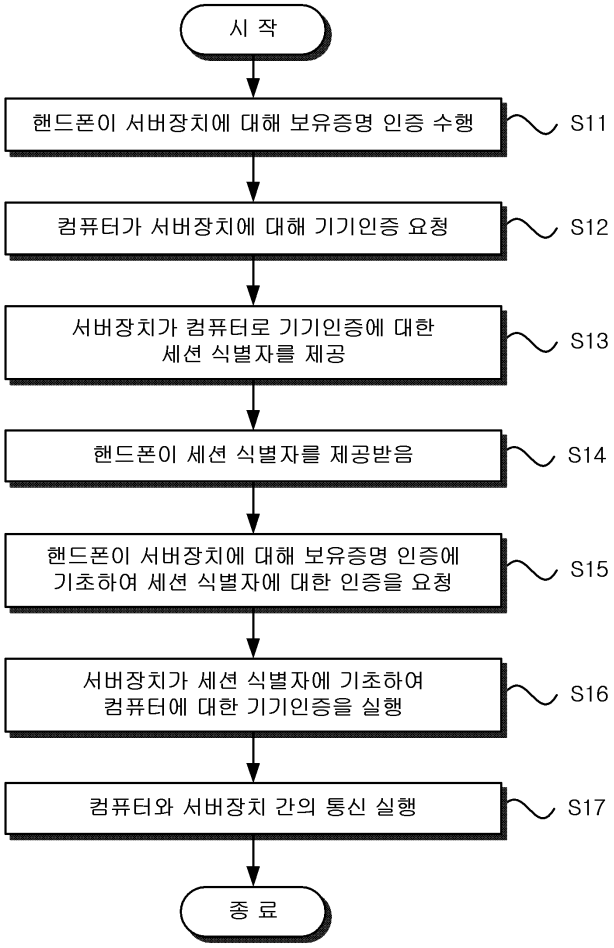
300: 서버장치

도면

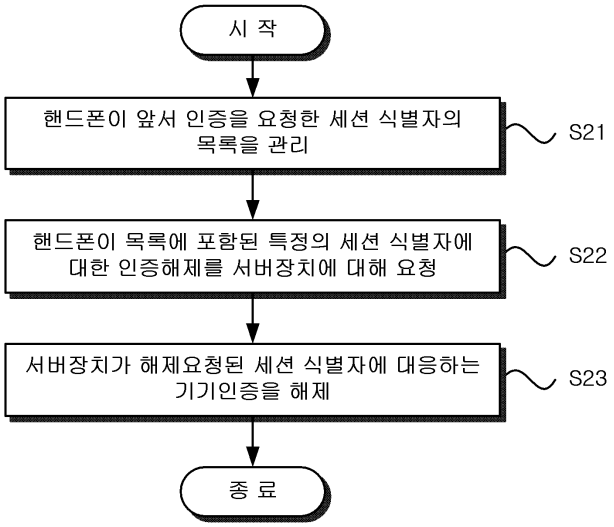
도면1


컴퓨터(200)
핸드폰(100)
서버장치(300)
보유증명 인증
웹사이트 접속을 위한 기기인증 요청
기기인증에 대한 세션 식별자 제공
세션 식별자 제공
세션 식별자에 대한
인증 요청
컴퓨터 기기인증
기기인증에 따른 통신
세션 식별자
목록 관리
특정 세션 식별자에 대한
인증 해제 요청
기기인증 해제
위치정보 저장
이격 판단
인증 해제 요청
기기인증 해제

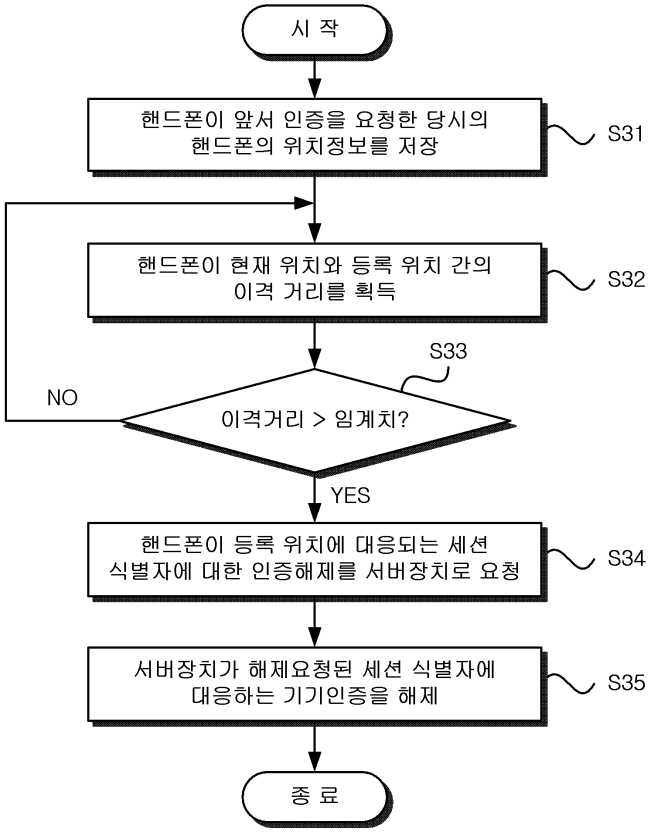
도면2


시 작
핸드폰이 서버장치에 대해 보유증명 인증 수행
S11
컴퓨터가 서버장치에 대해 기기인증 요청
S12
서버장치가 컴퓨터로 기기인증에 대한 세션 식별자를 제공
S13
핸드폰이 세션 식별자를 제공받음
S14
핸드폰이 서버장치에 대해 보유증명 인증에 기초하여 세션 식별자에 대한 인증을 요청
S15
서버장치가 세션 식별자에 기초하여 컴퓨터에 대한 기기인증을 실행
S16
컴퓨터와 서버장치 간의 통신 실행
S17
종 료

도면3


시 작
핸드폰이 앞서 인증을 요청한 세션 식별자의 목록을 관리
S21
핸드폰이 목록에 포함된 특정의 세션 식별자에 대한 인증해제를 서버장치에 대해 요청
S22
서버장치가 해제요청된 세션 식별자에 대응하는 기기인증을 해제
S23
종 료

도면4


시 작
핸드폰이 앞서 인증을 요청한 당시의
핸드폰의 위치정보를 저장
S31
핸드폰이 현재 위치와 등록 위치 간의
이격 거리를 획득
S32
S33
NO
이격거리 > 임계치?
YES
핸드폰이 등록 위치에 대응되는 세션
식별자에 대한 인증해제를 서버장치로 요청
S34
서버장치가 해제요청된 세션 식별자에
대응하는 기기인증을 해제
S35
종 료